



This is a digital copy of a book that was preserved for generations on library shelves before it was carefully scanned by Google as part of a project to make the world's books discoverable online.

It has survived long enough for the copyright to expire and the book to enter the public domain. A public domain book is one that was never subject to copyright or whose legal copyright term has expired. Whether a book is in the public domain may vary country to country. Public domain books are our gateways to the past, representing a wealth of history, culture and knowledge that's often difficult to discover.

Marks, notations and other marginalia present in the original volume will appear in this file - a reminder of this book's long journey from the publisher to a library and finally to you.

Usage guidelines

Google is proud to partner with libraries to digitize public domain materials and make them widely accessible. Public domain books belong to the public and we are merely their custodians. Nevertheless, this work is expensive, so in order to keep providing this resource, we have taken steps to prevent abuse by commercial parties, including placing technical restrictions on automated querying.

We also ask that you:

- + *Make non-commercial use of the files* We designed Google Book Search for use by individuals, and we request that you use these files for personal, non-commercial purposes.
- + *Refrain from automated querying* Do not send automated queries of any sort to Google's system: If you are conducting research on machine translation, optical character recognition or other areas where access to a large amount of text is helpful, please contact us. We encourage the use of public domain materials for these purposes and may be able to help.
- + *Maintain attribution* The Google "watermark" you see on each file is essential for informing people about this project and helping them find additional materials through Google Book Search. Please do not remove it.
- + *Keep it legal* Whatever your use, remember that you are responsible for ensuring that what you are doing is legal. Do not assume that just because we believe a book is in the public domain for users in the United States, that the work is also in the public domain for users in other countries. Whether a book is still in copyright varies from country to country, and we can't offer guidance on whether any specific use of any specific book is allowed. Please do not assume that a book's appearance in Google Book Search means it can be used in any manner anywhere in the world. Copyright infringement liability can be quite severe.

About Google Book Search

Google's mission is to organize the world's information and to make it universally accessible and useful. Google Book Search helps readers discover the world's books while helping authors and publishers reach new audiences. You can search through the full text of this book on the web at <http://books.google.com/>

01 04 1508.71



VORLESUNGEN
ÜBER
ZAHLENTHEORIE

VON
P. G. LEJEUNE DIRICHLET.

©

VORLESUNGEN

ÜBER

ZAHLENTHEORIE

VON

Peter Gustav
P. G. LEJEUNE DIRICHLET.

HERAUSGEGEBEN

UND

MIT ZUSÄTZEN VERSEHEN

VON

Richard
R. DEDEKIND,

Professor der höheren Mathematik am Collegium Carolinum zu Braunschweig.

Z W E I T E

UMGEARBEITETE UND VERMEHRTE AUFLAGE.

BRAUNSCHWEIG,

DRUCK UND VERLAG VON FRIEDRICH VIEWEG UND SOHN.

1 8 7 1.

Math 1508.71

HARVARD COLLEGE LIBRARY

1872, Nov. 29,

Haven Fund.

Die Herausgabe einer Uebersetzung in französischer und englischer Sprache,
sowie in anderen modernen Sprachen wird vorbehalten.

395
46-166
20

VORWORT DES HERAUSGEBERS.

Gleich nach dem Tode *Dirichlet's* wurde ich mehrfach aufgefordert, die von ihm gehaltenen Universitäts-Vorlesungen, welche so ausserordentlich viel zur Verbreitung der Bekanntschaft mit neueren und feineren Theilen der Mathematik beigetragen haben, in möglichst getreuer Form zu veröffentlichen; ich glaubte dieser Aufforderung um so eher nachkommen zu können, als ich in den Jahren 1855 bis 1858 die wichtigsten dieser Vorlesungen in Göttingen gehört und ausserdem vielfach Gelegenheit gehabt hatte, im persönlichen Verkehr *Dirichlet's* Gründe für die von ihm befolgte Methode des Vortrags kennen zu lernen. Nachdem auch die Verwandten *Dirichlet's* mich dazu ermächtigt haben, so übergebe ich dem mathematischen Publicum hiermit eine Ausarbeitung der Vorlesung über Zahlentheorie, bei welcher im Wesentlichen der im Winter 1856 bis 1857 von *Dirichlet* befolgte Gang eingehalten ist; er selbst fasste damals den Gedanken einer Herausgabe dieser Vorlesungen, und da er seinen

Vortrag nie schriftlich ausgearbeitet hatte, so diente ihm ein von mir geschriebenes, allerdings nur die Hauptmomente der Beweise enthaltendes Heft dazu, einen ungefähren Ueberschlag über die Ausdehnung der einzelnen Abschnitte zu machen. In öfter wiederkehrenden Gesprächen über diesen Plan äusserte er die Absicht, bei der Veröffentlichung manche Abschnitte hinzufügen zu wollen, die in einem Lehrbuch nicht fehlen dürften, die aber in jener Wintervorlesung aus Mangel an Zeit übergangen werden mussten. Bei der jetzigen Herausgabe ist daher im Wesentlichen zwar das eben erwähnte Heft zu Grunde gelegt, aber ich habe theils nach älteren Heften, theils nach *Dirichlet'schen* Abhandlungen, endlich auch ganz nach eigenem Ermessen Zusätze von nicht unbedeutender Ausdehnung gemacht, welche ich hier anführen zu müssen glaube, um für sie die Verantwortlichkeit zu übernehmen; sie sind in den Paragraphen 105 bis 110, 121 bis 144 und in den unmittelbar unter den Text gesetzten Anmerkungen enthalten.

Es ist meine Absicht, diesem ersten Bande, dessen Vollendung durch andere Arbeiten sich bis jetzt verzögert hat, zunächst einen zweiten weniger umfangreichen nachfolgen zu lassen, in welchem die Vorlesung über die im umgekehrten Verhältniss des Quadrats der Entfernung wirkenden Kräfte wiedergegeben werden soll.

Braunschweig, im October 1863.

R. Dedekind.

VORWORT ZUR ZWEITEN AUFLAGE.

Diese neue Auflage unterscheidet sich von der ersten hauptsächlich dadurch, dass sie um das zehnte Supplement bereichert ist, welches von der Composition der Formen handelt. Dieser Gegenstand war bei der ersten Auflage gänzlich ausgeschlossen geblieben, weil die einzige Abhandlung *Dirichlet's*, welche sich unmittelbar hierauf bezieht, nur den ersten Fundamentalsatz behandelt, weshalb ich befürchten musste, bei einer vollständigen Darstellung dieser Theorie mich zu weit von dem ursprünglichen Zwecke der Herausgabe zu entfernen. Obwohl ich nun diese Gefahr auch jetzt durchaus nicht verkenne, so habe ich mich doch aus vielen Gründen entschlossen, das zehnte Supplement hinzuzufügen und dadurch mehrfachen an mich gerichteten Aufforderungen nach besten Kräften zu entsprechen, hauptsächlich, weil trotz des ungemeinen Interesses und der steigenden Wichtigkeit dieser Theorie noch immer kein Versuch gemacht ist, die grossen Schwierigkeiten hinwegzuräumen, welche beim Eindringen

in dieselbe sich dem Anfänger entgegenstellen, und weil die übrigen Abschnitte des Werkes ganz vorzüglich geeignet sind, einen solchen Versuch zu erleichtern. Bei der wirklichen Ausführung dieses Entschlusses habe ich mich nicht auf die Begründung der ersten Elemente beschränkt, sondern es für nothwendig gehalten, den grössten Theil der in der fünften Section der *Disquisitiones Arithmeticae* enthaltenen Untersuchungen möglichst kurz und einfach zur Darstellung zu bringen. Endlich habe ich in dieses Supplement eine allgemeine Theorie der *Ideale* aufgenommen, um auf den Hauptgegenstand des ganzen Buches von einem höheren Standpunkte aus ein neues Licht zu werfen; hierbei habe ich mich freilich auf die Darstellung der Grundlagen beschränken müssen, doch hoffe ich, dass das Streben nach charakteristischen Grundbegriffen, welches in anderen Theilen der Mathematik mit so schönen Erfolgen gekrönt ist, mir nicht ganz missglückt sein möge. Die Untersuchungen in diesem von *Kummer* geschaffenen Gebiete, welche *Kronecker* vor vierzehn Jahren angestellt hat, sind bis jetzt nicht veröffentlicht, und ich vermag nach den damaligen brieflichen Mittheilungen dieses ausgezeichneten Mathematikers nicht zu beurtheilen, in welchen Beziehungen seine Principien zu den meinigen stehen. Der Aufbau der Theorie in §. 163 befriedigt mich selbst zwar noch nicht vollständig; allein es ist mir erst nach sehr langem Nachdenken gelungen, ihm diese Form zu geben, während ich vor etwa zehn Jahren von der Theorie der höheren Congruenzen in Verbindung mit den Principien von *Galois* zu einer ganz anderen Begründungsart gelangt war, welche einige

Berührungspunkte mit der Theorie der idealen Zahlen von *Selling* hat, mir aber jetzt weniger naturgemäss erscheint. Eine ausführlichere Darstellung der an den Begriff eines *Körpers* (§. 159) sich anschliessenden algebraischen Principien, welche hier nur beiläufig angedeutet werden konnten, verspare ich mir für eine andere Gelegenheit.

Es ist natürlich, dass die Hinzufügung des zehnten Supplementes einige Rückwirkung auf die früheren Abschnitte ausgeübt hat; doch braucht man nicht zu besorgen, dass ich mich durch solche Abänderungen der ersten Auflage im Plan und in der Haltung der Darstellung von der eigentlichen Grundlage, den Vorlesungen *Dirichlet's*, weiter entfernt habe. Um einem etwaigen Vorwurfe dieser Art von vornherein zu begegnen, wiederhole ich hier (aus den Göttinger Gelehrten Anzeigen vom 27. Januar 1864), dass auch die erste Auflage sich nicht auf ein in den Vorlesungen selbst nachgeschriebenes Heft, sondern nur auf Notizen stützt, welche ich aus der Erinnerung und grösstentheils in äusserst kurzer Form verfasst habe; als ich diese Vorlesungen als Privatdocent in Göttingen hörte, war ich mit dem Stoffe hinreichend vertraut, und mein Hauptzweck bestand darin, den überaus eindringlichen Vortrag *Dirichlet's* vollständig auf mich wirken zu lassen. Bei der Herausgabe der ersten Auflage, welche erst nach einer Reihe von Jahren erfolgte, wurde es nothwendig, diese Notizen ganz neu auszuarbeiten und auch durch eigene Zuthaten (z. B. §. 2, wenn ich nicht irre) zu ergänzen, die unmöglich alle erwähnt werden konnten. Aber damals sowohl wie jetzt

ist es mein eifrigstes Streben gewesen, *Dirichlet's* Vortrag mit grösster Treue wiederzugeben. Volle Freiheit habe ich mir dagegen bei den eigenen Zusätzen gestattet; gänzlich umgearbeitet sind z. B. die §§. 105 bis 110, 143, 144, und manches Neue ist theils im Text, theils in Form von Noten hinzugefügt.

Endlich habe ich mich bemüht, überall, wo es mir möglich war, auf die Quellen zu verweisen, um den Leser zum Studium der Originalwerke zu veranlassen und in ihm ein Bild von den Fortschritten der Wissenschaft zu erwecken, deren ebenso tiefe wie erhabene Wahrheiten einen Schatz bilden, welcher die unvergängliche Frucht eines wahrhaft edelen Wettkampfes der europäischen Völker ist.

Braunschweig, 1. März 1871.

R. Dedekind.

Erster Abschnitt.

Von der Theilbarkeit der Zahlen.

§. 1.

Wir behandeln in diesem Abschnitte einige arithmetische Sätze, welche man zwar in den meisten Lehrbüchern vorfindet, die aber für unsere Wissenschaft von so fundamentaler Bedeutung sind, dass eine strenge Begründung derselben hier durchaus nothwendig erscheint. Dahin gehört zuerst der Satz, dass das Product einer Reihe von ganzen positiven Zahlen unabhängig von der Anordnung ist, in welcher man die Multiplication ausführt. Indem wir uns zunächst auf den Fall beschränken, in welchem es sich um *drei* Zahlen a, b, c handelt, bilden wir das folgende Schema

$$\begin{array}{ccccccc} c, & c, & c, & c & \dots & c \\ c, & c, & c, & c & \dots & c \\ c, & c, & c, & c & \dots & c \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \\ c, & c, & c, & c & \dots & c \end{array}$$

welches aus b Horizontalreihen besteht, deren jede die Zahl c gleich oft, nämlich a mal enthält, und stellen uns die Aufgabe, die Summe aller aufgeschriebenen Zahlen zu bestimmen. Zunächst können wir sagen: da die Zahl c in jeder Horizontalreihe a mal vorkommt, so ist nach dem Grundbegriff der Multiplication die

anderes Mal als $(2 + \sqrt{-11}) (2 - \sqrt{-11})$ darstellen, obgleich jede der vier Zahlen

$$3, 5, 2 + \sqrt{-11}, 2 - \sqrt{-11}$$

nicht weiter in Factoren von der Form $t + u\sqrt{-11}$ zerlegbar ist. Der Grund dieser interessanten Erscheinung liegt allein darin, dass es bei den Zahlen dieser Form nicht mehr gelingt, einen nach einer endlichen Anzahl von Operationen abschliessenden Algorithmus zur Auffindung der gemeinschaftlichen Divisoren zweier Zahlen zu bilden*).

*) Die Einführung der ganzen complexen Zahlen von der Form $t + u\sqrt{-1}$ rührt von *Gauss* her; eine kurze Darstellung der Elemente dieser neuen Zahlentheorie findet man in seiner Abhandlung *Theoria residuorum biquadraticorum* II, oder in einer Abhandlung von *Dirichlet*: *Recherches sur les formes quadratiques à coefficients et à indéterminées complexes* (Crelle's Journal XXIV). Das oben erwähnte abweichende Verhalten anderer Zahlformen hat *Kummer* zur Einführung der *idealen* Zahlen veranlasst (Crelle's Journal XXXV).

$$1 \cdot 2 \cdot 3 \dots (p-1) + 1$$

durch p theilbar, so muss p eine Primzahl sein; wäre nämlich p eine zusammengesetzte Zahl, also ausser durch 1 und durch sich selbst auch noch durch eine andere Zahl a theilbar, so würde a nothwendig eine der Zahlen $2, 3 \dots (p-1)$ sein müssen; da nun die obige Summe und ihr erstes Glied durch a theilbar ist, so müsste auch das zweite Glied 1 durch a theilbar sein, was nicht möglich ist.

Einen andern interessanten Satz erhält man durch Anwendung des dritten der vorhergehenden Sätze auf dasselbe Beispiel. Bezeichnet nämlich δ irgend einen Divisor von $p-1$, so ist bekanntlich

$$x^{p-1} - 1 = (x^\delta - 1) \psi(x),$$

wo $\psi(x)$ ein Polynom mit ganzen Coefficienten bedeutet. Hieraus folgt also: *Die Congruenz*

$$x^\delta \equiv 1 \pmod{p},$$

deren Grad δ ein Divisor von $p-1$ ist, besitzt stets δ incongruente Wurzeln.

§. 28.

Der zuletzt abgeleitete Satz gehört seinem Inhalte nach eigentlich in eine allgemeinere Theorie, nämlich in die Theorie der *binomischen Congruenzen* von der Form

$$ax^n \equiv b \pmod{k}.$$

Dieselbe stützt sich auf die Betrachtung der sogenannten *Potenzreste*, d. h. der Reste der successiven Potenzen einer Zahl, und wir beschäftigen uns daher zunächst mit der Untersuchung der interessanten Gesetze, welche hier hervortreten.

Es sei also k ein beliebiger Modul, und a relative Primzahl gegen denselben; bilden wir nun die Reihe

$$1, a, a^2, a^3 \dots$$

der successiven Potenzen von a und setzen dieselbe hinreichend weit fort, so muss es einmal geschehen, dass zwei verschiedene Glieder a^s und a^{s+n} einander nach dem Modul k congruent werden; denn es giebt ja nur eine endliche Anzahl incongruenter Zahlen. Aus der Congruenz

zu lösen, so wird man, indem man wieder die primitive Wurzel 2 zur Basis des Indexsystems wählt,

$$\text{Ind. } x \equiv \text{Ind. } 6 - \text{Ind. } 5 \equiv 5 - 9 \equiv 8 \pmod{12}$$

und folglich

$$x \equiv 9 \pmod{13}$$

finden.

Diese Methode, Congruenzen ersten Grades aufzulösen, scheint auf den ersten Blick nur dann anwendbar, wenn der Modul eine Primzahl ist; allein man kann leicht zeigen, dass jede beliebige Congruenz ersten Grades

$$ax \equiv b \pmod{k},$$

deren Modul eine zusammengesetzte Zahl ist, auf eine Kette von Congruenzen reducirt werden kann, deren Moduln Primzahlen sind. Wir können uns hierbei auf den Fall beschränken, in welchem a relative Primzahl gegen k ist. Man löse nun zuerst die Congruenz

$$ax \equiv b \pmod{p},$$

wo p irgend eine in $k = pk'$ aufgehende Primzahl ist, nach der neuen Methode, so erhält man ein Resultat von der Form

$$x \equiv \alpha \pmod{p} \quad \text{oder} \quad x = \alpha + px',$$

wo x' eine beliebige ganze Zahl ist; substituirt man diesen Ausdruck in die gegebene Congruenz, so nimmt sie die folgende Form an:

$$pax' \equiv b - a\alpha \pmod{k}.$$

Da nun $b - a\alpha$ durch p theilbar, also von der Form $b'p$ ist, so stimmen sämtliche Wurzeln der vorstehenden Congruenz mit den sämtlichen Wurzeln der Congruenz

$$ax' \equiv b' \pmod{k'}$$

überein. Auf dieselbe Weise kann man nun fortfahren, indem man diese Congruenz zunächst nur in Bezug auf eine in k' aufgehende Primzahl p' löst, u. s. f.; man braucht dann zuletzt nur noch von der Wurzel der letzten dieser Congruenzen durch successive Substitution zu der ursprünglichen überzugehen.

§. 31.

Wir benutzen nun noch die Theorie der Indices, um auf sie die Theorie der *binomischen Congruenzen* für einen Primzahl-

modulus p zu stützen; nach einer frühern Bemerkung kann man einer jeden solchen binomischen Congruenz die Form

$$x^n \equiv D \pmod{p} \quad (1)$$

geben, in welcher der Coefficient der Potenz der Unbekannten $= 1$ ist; da ferner der Fall, in welchem $D \equiv 0 \pmod{p}$ und folglich auch $x \equiv 0 \pmod{p}$, ohne Interesse ist, so schliessen wir denselben aus.

Bezeichnen wir nun zur Abkürzung die Indices von D und x resp. mit γ und ξ (wenn irgend eine primitive Wurzel g von p zur Basis genommen ist), so reducirt sich die Auflösung der Congruenz (1) auf die Bestimmung aller Wurzeln ξ der Congruenz ersten Grades

$$n\xi \equiv \gamma \pmod{p-1}; \quad (2)$$

denn offenbar entspricht jeder Wurzel der einen dieser beiden Congruenzen (1) und (2) auch stets eine und nur eine Wurzel der andern.

Es sei jetzt δ der grösste gemeinschaftliche Divisor der Zahlen $p-1$ und n , so ist (§. 22) die Congruenz (2) nur dann möglich, wenn die Bedingung

$$\gamma \equiv 0 \pmod{\delta} \quad (3)$$

erfüllt ist, und dann hat sie δ nach dem Modul $p-1$ incongruente Wurzeln ξ . Wir schliessen hieraus unmittelbar den Satz:

Ist δ der grösste gemeinschaftliche Divisor des Grades n der Congruenz (1) und der Zahl $p-1$, so ist diese Congruenz nur dann möglich, wenn die Bedingung

$$\text{Ind. } D \equiv 0 \pmod{\delta} \quad (4)$$

erfüllt ist, und dann besitzt sie δ nach dem Modul p incongruente Wurzeln x .

Liegt z. B. die Congruenz

$$x^8 \equiv 3 \pmod{13}$$

vor, so ist $\delta = 4$; nehmen wir ferner die primitive Wurzel 2 als Basis für die Indices, so ist $\text{Ind. } 3 = 4$, also ist die Bedingung (4) erfüllt, und die vorgelegte Congruenz hat 4 nach dem Modul 13 incongruente Wurzeln; um diese zu finden, bilden wir die Congruenz ersten Grades

$$8\xi \equiv 4 \pmod{12} \quad \text{oder} \quad 2\xi \equiv 1 \pmod{3},$$

und erhalten hieraus

$$\xi \equiv 2 \pmod{3}$$

oder

$$\xi \equiv 2, \text{ oder } 5, \text{ oder } 8, \text{ oder } 11 \pmod{12},$$

folglich, indem wir zu diesen Indices ξ die zugehörigen Zahlen suchen,

$$x \equiv 4, \text{ oder } 6, \text{ oder } 9, \text{ oder } 7 \pmod{13}.$$

Da die Möglichkeit der binomischen Congruenz von der Wahl der primitiven Wurzel g , auf welche sich die Indices γ und ξ beziehen, nothwendig unabhängig sein muss, so wird das Kriterium, dass der Index γ einer Zahl D durch einen Divisor δ der Zahl $p-1$ theilbar sein muss, in eine von der Theorie der Indices unabhängige Form gebracht werden können. Dies bestätigt sich auf folgende Weise. Sobald in Bezug auf irgend eine Basis g der Index γ der Zahl D durch den Divisor δ von $p-1$ theilbar, also von der Form $h\delta$ ist, so haben wir die Congruenz

$$D \equiv g^{h\delta} \pmod{p}$$

und hieraus durch Potenzirung

$$D^{\frac{p-1}{\delta}} \equiv g^{h(p-1)} \equiv 1 \pmod{p};$$

und umgekehrt, sobald die Zahl D dieser Bedingung

$$D^{\frac{p-1}{\delta}} \equiv 1 \pmod{p}$$

genügt, muss der in Bezug auf eine beliebige Basis g genommene Index γ der Zahl D durch δ theilbar sein; denn es sei

$$D \equiv g^\gamma \pmod{p},$$

so folgt hieraus

$$g^{\gamma \cdot \frac{p-1}{\delta}} \equiv 1 \pmod{p},$$

und da g eine primitive Wurzel, d. h. eine zum Exponenten $p-1$ gehörende Zahl ist, so muss der Exponent durch $p-1$, und folglich der Index γ durch δ theilbar sein.

Nachdem das ursprüngliche Kriterium so umgeformt ist, können wir unsern Satz in folgender Weise unabhängig von der Theorie der Indices aussprechen:

Ist δ der grösste gemeinschaftliche Divisor der Zahlen n und $p-1$, so hat die Congruenz

$$x^n \equiv D \pmod{p}, \tag{1}$$

genau δ incongruente Wurzeln, oder gar keine, je nachdem die Zahl D der Bedingung

$$D^{\frac{p-1}{\delta}} \equiv 1 \pmod{p} \quad (5)$$

genügt oder nicht genügt.

Den speciellen Fall, in welchem $\delta = n$ und $D = 1$ ist, haben wir schon früher (§. 27) auf anderm Wege bewiesen; es würde nicht schwer sein, aus den dort angewandten Principien auch den allgemeinen Satz abzuleiten, ohne die Theorie der Indices zu Hülfe zu rufen; doch überlassen wir der Kürze halber diese Untersuchung dem Leser.

Wir können nun auch noch die Frage aufstellen: wenn der Grad n der Congruenz (1) gegeben ist, wie viele incongruente Zahlen D existiren, für welche die Congruenz (1) möglich ist? Hierauf liefert der Satz selbst sogleich die Antwort, denn diese Zahlen D sind ja die sämtlichen Wurzeln der binomischen Congruenz

$$x^{\frac{p-1}{\delta}} \equiv 1 \pmod{p};$$

der grösste gemeinschaftliche Divisor des Exponenten $(p-1):\delta$ und der Zahl $p-1$ ist in diesem Falle der Exponent $(p-1):\delta$ selbst, und da das Kriterium für die Möglichkeit offenbar erfüllt ist, so ist also die Anzahl aller incongruenten Zahlen D , für welche die Congruenz (1) möglich ist, genau $= (p-1):\delta$. Man nennt solche Zahlen D , welche einer n ten Potenz einer Zahl congruent sind, kurz n te Potenzreste, und wir können daher sagen:

Die Anzahl aller n ten Potenzreste ist $= (p-1):\delta$, wo δ den grössten gemeinschaftlichen Divisor der Zahlen n und $p-1$ bezeichnet.

Man findet dieselben offenbar, wenn man alle incongruenten Zahlen zur n ten Potenz erhebt und deren Reste bildet. Wenn $n = 2, 3, 4$ ist, so nennt man diese Zahlen resp. *quadratische, cubische, biquadratische Reste*. Mit der Theorie der erstern, welche für sich allein schon eine grosse Ausdehnung besitzt, werden wir uns nun im Folgenden ausführlich beschäftigen.

Dritter Abschnitt.

Von den quadratischen Resten.

§. 32.

Wir behandeln im Folgenden ausführlich die Theorie der Congruenzen von der Form

$$x^2 \equiv D \pmod{k}, \quad (1)$$

in welcher wir stets D als *relative Primzahl* gegen den Modul k voraussetzen. Es würde sich leicht zeigen lassen, dass jede beliebige Congruenz zweiten Grades auf diesen Fall zurückgeführt werden kann; doch wollen wir uns dabei nicht aufhalten. So oft nun die Congruenz (1) möglich ist, d. h. so oft sie Wurzeln hat, heisst die Zahl D *quadratischer Rest der Zahl k* ; im entgegengesetzten Fall heisst D *quadratischer Nichtrest der Zahl k* . Man lässt auch häufig, wenn kein Missverständniss zu befürchten ist, das Beiwort „quadratisch“ fort und nennt kurz die Zahl D *Rest* oder *Nichtrest* von k , je nachdem die Congruenz (1) möglich ist oder nicht. Unmittelbar leuchtet hieraus ein, dass zwei nach dem Modul k congruente Zahlen entweder beide Reste von k , oder beide Nichtreste von k sind; d. h. alle in einer und derselben *Classe* enthaltenen Zahlen haben denselben Charakter; je nachdem eine von ihnen Rest oder Nichtrest des Modul k ist, sind sie alle Reste oder alle Nichtreste von k .

die positive oder negative Einheit, je nachdem die durch die Primzahl p nicht theilbare Zahl m quadratischer Rest oder Nichtrest von p ist; es ist daher stets

$$\left(\frac{m}{p}\right) \left(\frac{m}{p}\right) = +1 \quad \text{und} \quad m^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \pmod{p}.$$

Den Satz über den Charakter eines Productes kann man dann offenbar durch die folgende Gleichung ausdrücken:

$$\left(\frac{mnl\dots}{p}\right) = \left(\frac{m}{p}\right) \left(\frac{n}{p}\right) \left(\frac{l}{p}\right) \dots$$

Es leuchtet ferner ein, dass, sobald $m \equiv n \pmod{p}$, auch

$$\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$$

sein wird.

§. 34.

Es ist nun interessant zu sehen, dass die soeben gewonnenen Sätze, welche zum Theil als Resultate einer ausgedehnten Theorie, wie der der binomischen Congruenzen, erscheinen, sich aus den ersten Principien auf einem ganz elementaren Wege ableiten lassen, der zugleich einen neuen Beweis des Wilson'schen und Fermat'schen Satzes liefern wird.

Es sei D irgend eine durch die (ungerade) Primzahl p nicht theilbare Zahl, und r irgend eine der Zahlen

$$1, 2, 3 \dots (p-1); \tag{1}$$

dann existirt in derselben Reihe stets eine und nur eine Zahl s von der Beschaffenheit, dass

$$rs \equiv D \pmod{p}$$

ist; denn diese Zahl s ist ja die Wurzel der Congruenz ersten Grades $rx \equiv D \pmod{p}$; je zwei solche Zahlen r und s der Reihe (1), deren Product $\equiv D$ ist, wollen wir *zusammengehörige* Zahlen nennen; offenbar ist durch eine dieser beiden Zahlen die andere ebenfalls bestimmt. Identisch können diese beiden Zahlen nur dann werden, wenn die Congruenz

$$x^2 \equiv D \pmod{p} \tag{2}$$

möglich ist. Danach theilen wir unsere Untersuchung in zwei Fälle ein.

Erstens: Die Congruenz (2) ist unmöglich. — Dann sind also je zwei zusammengehörige Zahlen von einander verschieden, und da zwei solche Paare stets identisch sind, sobald sie nur eine gemeinschaftliche Zahl haben, so zerfallen die sämtlichen $p - 1$ Zahlen (1) in $\frac{1}{2}(p - 1)$ solche Paare zusammengehöriger Zahlen, und folglich ist ihr Product

$$1 \cdot 2 \cdot 3 \dots (p - 1) \equiv D^{\frac{p-1}{2}} \pmod{p}. \quad (3)$$

Zweitens: Die Congruenz (2) ist möglich. — Dann existirt also auch in der Reihe (1) mindestens eine Zahl ϱ von der Beschaffenheit, dass $\varrho^2 \equiv D$; sehen wir zu, ob ausser ϱ in der Reihe (1) noch eine solche Zahl σ existirt; dann muss $\sigma^2 \equiv \varrho^2$, folglich $(\sigma - \varrho)(\sigma + \varrho)$ durch p theilbar sein; da wir σ verschieden von ϱ voraussetzen, so ist $\sigma - \varrho$ nicht theilbar durch p , folglich muss $\sigma + \varrho$ theilbar durch p , also $\sigma = p - \varrho$ sein; und in der That ist wirklich $(p - \varrho)^2 \equiv D$. Trennen wir nun diese beiden (wirklich ungleichen) Zahlen ϱ und $\sigma = p - \varrho$, deren Product $\varrho \sigma \equiv -\varrho^2 \equiv -D$ ist, von den übrigen der Reihe (1), so zerfallen die letztern in $\frac{1}{2}(p - 3)$ Paare zusammengehöriger Zahlen von der Beschaffenheit, dass jedes Paar aus zwei verschiedenen Zahlen besteht. Demnach ist in diesem Fall das Product aller Zahlen der Reihe (1):

$$1 \cdot 2 \cdot 3 \dots (p - 1) \equiv -D^{\frac{p-1}{2}} \pmod{p}. \quad (4)$$

Nun giebt es aber einen Fall, in welchem die Congruenz (2) stets möglich ist, nämlich den, in welchem $D = 1 = 1^2$; wir erhalten daher zunächst aus (4) den Satz von *Wilson*:

$$1 \cdot 2 \cdot 3 \dots (p - 1) \equiv -1 \pmod{p}, \quad (5)$$

und substituiren wir dies in die Congruenzen (3) und (4), so erhalten wir das Resultat, dass

$$D^{\frac{p-1}{2}} \equiv +1 \quad \text{oder} \quad \equiv -1 \pmod{p}$$

ist, je nachdem die Congruenz (2) möglich oder nicht möglich ist. Da endlich ein dritter Fall nicht existiren kann, so erhalten wir allgemein

$$D^{p-1} = (D^{\frac{p-1}{2}})^2 \equiv (\pm 1)^2 \equiv +1 \pmod{p},$$

also den Satz von *Fermat*.

Durch diese einfache Betrachtung sind wir also sogleich bis zu denselben Sätzen in der Theorie der quadratischen Reste ge-

langt, welche vorher aus der allgemeinen Theorie der binomischen Congruenzen abgeleitet waren.

§. 35.

Wir wenden uns jetzt zu der Untersuchung des Falls, in welchem der Modul k der quadratischen Congruenz

$$x^2 \equiv D \pmod{k}$$

die Potenz einer Primzahl p ist; dabei müssen wir den Fall, in welchem $p = 2$, gesondert von den übrigen behandeln, in welchen p eine ungerade Primzahl ist*).

Ist zunächst p eine ungerade Primzahl, und $k = p^\pi$, wo π irgend eine positive ganze Zahl bedeutet, und nehmen wir an, die Congruenz

$$x^2 \equiv D \pmod{p^\pi} \quad (1)$$

sei möglich, so überzeugt man sich leicht, dass sie im Ganzen *zwei* incongruente Wurzeln hat; denn ist α eine bestimmte, und x irgend eine Wurzel, so muss

$$x^2 - \alpha^2 = (x - \alpha)(x + \alpha) \equiv 0 \pmod{p^\pi}.$$

sein; von den beiden Factoren $x - \alpha$ und $x + \alpha$ ist aber nur einer durch p theilbar; denn wären beide durch p theilbar, so wäre auch ihre Differenz 2α , und folglich auch α durch p theilbar, was nicht der Fall ist, da wir $D \equiv \alpha^2$ als nicht theilbar durch p vorausgesetzt haben. Da also einer der beiden Factoren relative Primzahl gegen p^π ist, so muss der andere für sich allein durch p^π theilbar sein. Es ist daher entweder

$$x \equiv \alpha \pmod{p^\pi}, \quad \text{oder} \quad x \equiv -\alpha \pmod{p^\pi};$$

also hat die Congruenz (1) entweder gar keine Wurzel, oder sie hat zwei incongruente Wurzeln α und $-\alpha$.

Es ist nun noch zu entscheiden, wann das Eine, wann das Andere Statt finden wird. Da nun jede Wurzel α der Congruenz (1) auch eine Wurzel der Congruenz

$$x^2 \equiv D \pmod{p} \quad (2)$$

ist, so leuchtet ein, dass die Congruenz (1) nur dann möglich ist, wenn D quadratischer Rest von p ist; es fragt sich daher nur, ob

*) Die nachfolgenden Resultate lassen sich auch aus dem in §. 145 bewiesenen Satze ableiten.

